UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/050,274	01/16/2002	Yoon Seok Yang	2080-3-66	7037

35884 7590 01/12/2006

LEE, HONG, DEGERMAN, KANG & SCHMADEKA, P.C.
801 SOUTH FIQUEROA STREET
14TH FLOOR
LOS ANGELES, CA 90017

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 01/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/050,274	YANG, YOON SEOK	
	Examiner	Art Unit	
	Christopher J. Brown	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *24 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1 The applicant's argument recites that the references of Mroczkowski and Luyster do not teach a unit receiving a stream of data byte units. In response the examiner points out that although Luyster does not explicitly teach receiving a stream of byte units, it inherent that data is received streamed. Luyster simply teaches receiving "n-bit cipher input (eg plaintext)", (Col 18 line 54). Then forms the data into blocks. Data does not inherently arrive in preformed blocks. Also, if one substituted 8 for n, it would result in a 8-bit cipher input, or byte input.

The previous office action below is repeated for the applicant's convienience:

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 9, 10-14 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000) in view of Luyster (US 6,182,216).

Regarding claim 1, Mroczkowski discloses an apparatus implementing a block cipher comprising:

a control unit (encryption and decryption control, Figures 1 and 2);

a key schedule unit (key register, keyround, subkey buffer) carrying out a key schedule every round in accordance with a size and a key value of a block inputted from outside (key) so as to output a key value the encryption or decryption each round (subkey); and a block round unit (input register, encryption or decryption round, result buffer) receiving converted data of block units (input data) from the control unit, receiving the key value from the key schedule (key) so as to carry out the encryption or decryption, and outputting the encrypted or decrypted result (output data) to the control unit (Figures 1 and 2; section 2.1).

But Mroczkowski does not explicitly explain the control unit receiving a data stream of byte units, converting data stream into block data, and outputting the block data for encryption or decryption, the control unit receiving encrypted or decrypted block data, converting the received encrypted or decrypted block data into byte units, and outputting the converted block data of the byte units.

However, Luyster teaches an apparatus implementing a block cipher comprising a block control unit receiving a data stream of byte units (50), converting data stream into block data (segment), and outputting the block data for encryption or decryption, the control unit receiving encrypted or decrypted block data, converting the received encrypted or decrypted

block data into byte units, and outputting the converted block data of the byte units for the purpose of performing the operation of the block cipher on a large data set more efficiently in an iterative manner (Fig. 3 and 13; col. 2, lines 18-20 and 37-65; col. 18, lines 54-67; col. 23, lines 39-45; col. 45, lines 17-40; col. 57, lines 13-19).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the apparatus of Mroczkowski with the teaching of Luyster to provide a control unit receiving a data stream of byte units, converting data stream into block data, and outputting the block data for encryption or decryption, the control unit receiving encrypted or decrypted block data, converting the received encrypted or decrypted block data into byte units, and outputting the converted block data of the byte units. One would be motivated to do so in order to more efficiently process a large data set.

Regarding claim 2, the modified apparatus of Mroczkowski and Luyster is relied upon as applied to claim 1, and Mroczkowski and Luyster further teach an input buffer (Luyster, 50) storing the data stream of byte units and converting the received data stream into the block data (Luyster, 52; Mroczkowski, input data) having a predetermined size (Mroczkowski, 128 bits) so as to output the converted block data to the block round unit; and an output buffer (Luyster, 88) receiving the block data (Luyster, 84; Mroczkowski, output data) encrypted or decrypted in the block round unit and converting the received block data into the byte units so as to output a converted data (Luyster, Fig. 3; col. 18, lines 54-57; Mroczkowski, Figures 1 and 2, and section 2.1). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claim 3, the modified apparatus of Mroczkowski and Luyster is relied upon as applied to claim 2, and Mroczkowski and Luyster further teach an apparatus implementing a block cipher wherein a block round unit (Mroczkowski, Figures 1 and 2) completes all round calculation of data having been currently encrypted or decrypted before a next block data (Mroczkowski, input data) inputted from the control unit and then stores corresponding result in the output buffer of the control unit (Mroczkowski, section 2.1). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claim 4, the modified apparatus of Mroczkowski and Luyster is relied upon as applied to claim 1, and Mroczkowski and Luyster further teach that the key schedule unit carries every round the key schedule on a key required for the block round unit to process each round so as to output the key scheduled result the block round unit (Figures 1 and 2; section 2.1). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claim 9, the modified apparatus of Mroczkowski and Luyster is relied upon as applied to claim 1, and Mroczkowski and Luyster further teach that the control unit generates a control signal to produce the key value every round and then outputs the control signal to the key schedule unit (Mroczkowski, Figures 1 and 2, sections 2.1 and 2.2). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claims 10-14, 21-23, these claims are rejected for the same reasons as applied to claims 1-4 and 9. Therefore, such claims also would have been obvious.

Claims 5-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000) in view of Luyster (US 6,182,216) and further in view of Daemen et al. ("AES Proposal: Rijndael," March 1999), hereafter Daemen.

Regarding claim 5, the modified apparatus of Mroczkowski and Luyster is relied upon as applied to claim 4, and Mroczkowski and Luyster further teach a key selection unit for each round from selecting a 128 bit key required for each round so as to output the selected key to the block round unit (Mroczkowski, key for round selected from subkey buffer; Figures 1 and 2; section 2.1).

But Mroczkowski and Luyster do not explain that the key schedule unit comprises a key expansion unit expanding the inputted key value into a size amounting to {block size * (count of rounds + 1)}.

However, Luyster teaches an apparatus wherein the key schedule unit comprises a key expansion unit (Figures 5, 10 and 11; col. 51, lines 13-63) and also teaches that various key expansion algorithms are known in the art that are equally acceptable for implementation (col. 38, lines 58-64). Moreover, Daemen teaches a key expansion algorithm for the Rijndael block cipher wherein the key expansion unit expands the inputted key value into a size amounting to {block size * (count of rounds + 1)} (page 14, section 4.3.1) for the purpose of proposing a new encryption standard that is, among other things, efficient for use with 8-bit microprocessors (page 28, section 7.5).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the apparatus of Mroczkowski and Luyster with the further teaching of

Luyster and the teaching of Daemen to provide that the key schedule unit comprises a key expansion unit expanding the inputted key value into a size amounting to {block size * (count of rounds + 1)}. One would be motivated to do so in order to provide an encryption scheme that is efficient for use with low-end microprocessors, particularly where the key expansion scheme is employed for the same block cipher (Rijndael) implemented by Mroczkowski.

Regarding claim 6, this claim is rejected for the same reasons as applied to claim 5.

Regarding claim 7, the modified apparatus of Mroczkowski, Luyster, and Daemen is relied upon as applied to claim 5, and Mroczkowski, Luyster, and Daemen further teach that the key schedule unit comprises the key register amounting to the key value required substantially for one round (Luyster, registers K2 386 and K3 402, Figure 13; Mroczkowski, subkey buffer and key register, Figures 1 and 2). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claim 8, the modified apparatus of Mroczkowski, Luyster, and Daemen is relied upon as applied to claim 7, and Mroczkowski, Luyster, and Daemen further teach that the key register has a capacity amounting to {(size of an inputted block) * (size of one round)} (Daemen, section 4.3.2). Therefore, for the reasons applied above, such a claim also would have been obvious.

Regarding claims 15-20 and 24, these claims are rejected for the same reasons as applied to claims 5-8. Therefore, such claims also would have been obvious.

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

1/4/06

CJB

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100